# 24 hình thức lừa đảo trên không gian mạng Việt Nam

*Trước tình hình lừa đảo trực tuyến ngày càng gia tăng và trở nên phức tạp tại Việt Nam, ngày 23/6/2023, Bộ Thông tin và Truyền thông đã chính thức phát động "Tháng hành động tuyên truyền về nhận diện và phòng chống lừa đảo trực tuyến". Phân loại theo đặc điểm, các hình thức lừa đảo được chia thành 3 nhóm chính: giả mạo thương hiệu, chiếm đoạt tài khoản và các hình thức kết hợp khác. Cụ thể, đã có đến 24 hình thức lừa đảo được xác định đang hoạt động rầm rộ trên không gian mạng Việt Nam.*

Hướng đến việc nâng cao nhận thức và tạo sự cảnh giác cho người dân trước các hình thức lừa đảo trực tuyến, chi tiết về những hình thức này cùng với các biện pháp phòng chống hiệu quả sẽ được đề cập cụ thể trong hình ảnh dưới đây:

MỘT SỐ HÌNH THỨC
# LỪA ĐẢO
TRÊN KHÔNG GIAN MẠNG

INTERNET

## 24 HÌNH THỨC LỪA ĐẢO

### 1 "COMBO DU LỊCH GIÁ RẺ"

Lừa đảo chiếm đoạt tiền bạc, thông tin cá nhân qua các hình thức bẫy mua dịch vụ du lịch trọn gói

### 2 GIẢ MẠO BIÊN LAI CHUYỂN TIỀN THÀNH CÔNG

Các đối tượng lừa nạn nhân mua hàng số lượng lớn trên mạng xã hội. Làm giả biên lai chuyển tiền thành công bằng phần mềm

### 3 CUỘC GỌI VIDEO DEEPFAKE, DEEPVOICE

Các đối tượng sử dụng công nghệ trí tuệ nhân tạo (AI) để tạo ra những video hoặc hình ảnh giả, sao chép chân dung nhằm tạo ra các đoạn video giả người thân, bạn bè để thực hiện các cuộc gọi lừa đảo trực tuyến.

### 4 GIẢ DANH NHÂN VIÊN Y TẾ BÁO NGƯỜI THÂN ĐANG CẤP CỨU

Gọi điện thoại thông báo người thân đang nằm cấp cứu trong bệnh viện, yêu cầu chuyển tiền mổ gấp

### 5 TUYỂN NGƯỜI MẪU NHÍ

Lợi dụng mạng xã hội tiếp cận dụ dỗ các bậc phụ huynh có con trẻ đăng ký ứng tuyển người mẫu nhí. Yêu cầu nạn nhân đóng nhiều loại phí.

### 6 THÔNG BÁO "KHÓA SIM" VÌ CHƯA CHUẨN HÓA THUÊ BAO

Các đối tượng gọi điện thoại thông báo khóa dịch vụ viễn thông. Nạn nhân làm theo hướng dẫn sẽ bị lấy mất thông tin cá nhân.

### 7 GIẢ DANH CÔNG TY TÀI CHÍNH

Cung cấp khoản vay tiền với lãi suất thấp, thủ tục đơn giản. Yêu cầu nạn nhân đóng phí làm thủ tục rồi chiếm đoạt.

### 8 CÀI CẮM ỨNG DỤNG, LINK QUẢNG CÁO CỜ BẠC, CÁ ĐỘ, TÍN DỤNG ĐEN

Các đối tượng gài bẫy quảng cáo, ứng dụng cho vay. Nạn nhân sau khi cài đặt ứng dụng và cấp quyền cho ứng dụng truy cập điện thoại sẽ bị kẻ gian chiếm đoạt thông tin cá nhân.

### 9 GIẢ MẠO TRANG THÔNG TIN ĐIỆN TỬ, CƠ QUAN, DOANH NGHIỆP

Tạo trang web giả mạo có giao diện giống với trang web của các cơ quan, doanh nghiệp. Người dùng khai báo thông tin trên trang web giả sẽ bị đánh cắp thông tin cá nhân.

### 10 GIẢ MẠO SMS BRANDNAME, PHÁT TÁN TIN NHẮN GIẢ MẠO

Các đối tượng sử dụng trạm phát sóng BTS giả mạo để gửi hàng loạt tin nhắn lừa đảo tới người dùng. Nạn nhân làm theo hướng dẫn từ tin nhắn sẽ bị đánh cắp thông tin cá nhân.

### 11 LỪA ĐẢO ĐẦU TƯ CHỨNG KHOÁN, TIỀN ẢO, ĐA CẤP

Gửi Link thanh toán trực tuyến tham gia sàn giao dịch ảo, yêu cầu nạn nhân gửi tiền đặt cọc rồi chiếm đoạt.

### 12 ĐÁNH CẮP TÀI KHOẢN MXH, NHẮN TIN LỪA ĐẢO

Chiếm quyền đăng nhập vào tài khoản Facebook, Zalo nhắn tin cho bạn bè, người thân hỏi vay tiền.

### 13 LỪA ĐẢO TUYỂN CỘNG TÁC VIÊN ONLINE

Tuyển cộng tác viên "việc nhẹ lương cao" - giả mạo các trang sàn thương mại điện tử như Tiki, Shopee, Lazada và các thương hiệu lớn để chiếm đoạt tài sản của các nạn nhân.

### 14 RAO BÁN HÀNG GIẢ, HÀNG NHÁI TRÊN SÀN THƯƠNG MẠI ĐIỆN TỬ

Đăng tải quảng cáo mời chào người tiêu dùng mua hàng giả, hàng kém chất lượng không rõ nguồn gốc trên các sàn thương mại điện tử.

### 15 GIẢ DANH CƠ QUAN CÔNG AN, VIỆN KIỂM SÁT, TÒA ÁN

Các đối tượng giả danh cơ quan công an, viện kiểm sát, tòa án để gọi điện hăm dọa và sử dụng các chiêu trò lừa đảo nhằm chiếm đoạt tài sản của nạn nhân.

### 16 ĐÁNH CẮP TÀI KHOẢN MXH NHẮN TIN LỪA ĐẢO

Các đối tượng bẫy người dùng Internet khai báo thông tin CCCD trên các mẫu khảo sát. Từ đó sử dụng thông tin cá nhân đã đánh cắp để vay nợ tín dụng.

### 17 CHUYỂN NHẦM TIỀN VÀO TÀI KHOẢN NGÂN HÀNG

Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng và giả danh người thu hồi nợ để yêu cầu trả lại số tiền.

### 18 ĐÁNH CẮP TELEGRAM OTP

Lập tài khoản Telegram giả danh các cơ quan, tổ chức. Gửi tin nhắn yêu cầu xác thực tài khoản cho nạn nhân nhằm chiếm đoạt OTP để truy cập tài khoản của họ.

### 19 DỊCH VỤ LẤY LẠI TIỀN KHI ĐÃ BỊ LỪA

Giả danh nhân vật có uy tín, sức ảnh hưởng liên hệ cung cấp dịch vụ lấy lại tiền đã mất cho nạn nhân. Yêu cầu nạn nhân thanh toán trước hoặc cung cấp thông tin cá nhân.

### 20 DỊCH VỤ LẤY LẠI TÀI KHOẢN FACEBOOK

Tạo trang web quảng cáo dịch vụ lấy lại tài khoản Facebook. Yêu cầu người dùng cung cấp tiền cọc, thông tin cá nhân.

### 21 TUNG TIN GIẢ VỀ CUỘC GỌI MẤT TIỀN FLASHAI

Gọi điện thông báo tin giả, hướng dẫn phòng tránh cuộc gọi mất tiền FlashAI. Nạn nhân làm theo hướng dẫn sẽ bị chiếm đoạt thông tin cá nhân.

### 22 BẪY TÌNH CẢM, ĐẦU TƯ TÀI CHÍNH, GỬI BƯU KIỆN, TRÚNG THƯỞNG

Các đối tượng thông qua các mạng xã hội và ứng dụng hẹn hò tiếp cận người dùng. Lợi dụng tình cảm nạn nhân lừa chuyển tiền, kêu gọi đầu tư tài chính.

### 23 RẢI LINK PHISHING, SEEDING QUẢNG CÁO BÁN TRÊN MXH

Tạo trang web giả mạo ngân...

CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

# 3 KỸ NĂNG CƠ BẢN ĐỂ BẢO ĐẢM AN TOÀN THÔNG TIN CÁ NHÂN

## Hạn chế chia sẻ thông tin cá nhân

Hạn chế việc chia sẻ thông tin cá nhân của mình trên mạng, trừ khi chắc chắn rằng thông tin được sử dụng có kiểm soát. Hãy bảo đảm rằng bạn chỉ cung cấp thông tin cá nhân của mình cho cá nhân và tổ chức tin tưởng.

## Sử dụng mật khẩu an toàn

Sử dụng mật khẩu an toàn để bảo vệ tài khoản của mình trên mạng. Mật khẩu nên dài hơn 8 ký tự và bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt. Nên đổi mật khẩu thường xuyên và không nên sử dụng mật khẩu giống nhau cho nhiều tài khoản khác nhau.

## Chủ động nâng cao kiến thức bảo mật

Chủ động tìm hiểu về các phương thức bảo mật thông tin, cập nhật những tin tức mới nhất về các mối đe dọa bảo mật và học cách phòng ngừa chúng. Sử dụng các công cụ bảo mật như phần mềm chống virus và phần mềm chống đánh cắp thông tin để bảo vệ tài khoản của mình trên mạng.